2019

# Testbed-based Evaluation of SIEM Tool for Cyber Kill Chain Model in Power Grid SCADA System

Vivek Kumar Singh
*Iowa State University*, vsingh@iastate.edu

Steven Perez Callupe
*Iowa State University*

Manimaran Govindarasu
*Iowa State University*, gmani@iastate.edu

# Testbed-based Evaluation of SIEM Tool for Cyber Kill Chain Model in Power Grid SCADA System


## Abstract

Development of a smarter electric grid necessitates addressing the associated cyber security challenges. Since the interdependence between the legacy grid infrastructure and advanced information technology is growing rapidly, there are numerous ways advanced, motivated, and persistent attackers can affect the SCADA based critical infrastructure. Hence, developing a security information and event management (SIEM) is crucial for securing the SCADA power system. This paper presents the application of Security Onion (SecOn) to develop the network security monitoring (NSM) and intrusion detection system (IDS) in the context of SCADA cyber physical security. Initially, we have applied a cyber kill-chain model to demonstrate the different stages of attacks and associated mechanisms. Later, the rulebased IDS (RIDS) is developed using Snort IDS, and tested in the cyber-physical SCADA environment. Furthermore, we have evaluated its performance in terms of accuracy and detection latency. Our experimental results reveal that the SecOn tool is efficient in monitoring and detecting attacks within an acceptable time frame with a high accuracy rate.



## Disciplines

Electrical and Computer Engineering

## Comments

This proceeding is published as Singh, Vivek Kumar, Steven Perez Callupe, and Manimaran Govindarasu. "Testbed-based Evaluation of SIEM Tool for Cyber Kill Chain Model in Power Grid SCADA System." (2019). Posted with permission.

# Testbed-based Evaluation of SIEM Tool for Cyber Kill Chain Model in Power Grid SCADA System

Vivek Kumar Singh, Steven Perez Callupe, Manimaran Govindarasu
Department of Electrical and Computer Engineering, Iowa State University, Ames, IA 50011
Email:vsingh@iastate.edu, svperez@iastate.edu, gmani@iastate.edu

***Abstract*—Development of a smarter electric grid necessitates addressing the associated cyber security challenges. Since the interdependence between the legacy grid infrastructure and advanced information technology is growing rapidly, there are numerous ways advanced, motivated, and persistent attackers can affect the SCADA based critical infrastructure. Hence, developing a security information and event management (SIEM) is crucial for securing the SCADA power system. This paper presents the application of Security Onion (SecOn) to develop the network security monitoring (NSM) and intrusion detection system (IDS) in the context of SCADA cyber physical security. Initially, we have applied a cyber kill-chain model to demonstrate the different stages of attacks and associated mechanisms. Later, the rule-based IDS (RIDS) is developed using Snort IDS, and tested in the cyber-physical SCADA environment. Furthermore, we have evaluated its performance in terms of accuracy and detection latency. Our experimental results reveal that the SecOn tool is efficient in monitoring and detecting attacks within an acceptable time frame with a high accuracy rate.**

## I. INTRODUCTION

Today's power grid consists of a highly sophisticated, complex network where numerous controllers are performing several operations at the substation and control center levels to maintain the stability and reliability of the power system. It relies on the SCADA infrastructure for real-time monitoring, logging, report generation and automated control. The SCADA system is designed to stand up to the evolving grid given a little attention to cyber physical security which has exposed it to the multitude of vulnerabilities; and can be exploited by a human or malicious software. On July 2018, the Department of Homeland Security (DHS) has issued warning alerts against international threat actors, who have constantly targeted industrial control system (ICS) in the past [1]. Recently, the published reports by Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) discuss several cyber security incidents that have targeted the SCADA ICS including Stuxnet and the Ukraine's grid hack [2]. Based on the cyber-security surveys in [3], it was observed that the majority of attacks have affected normal operation, attacks are happening at different stages, the frequency of attacks has increased with time; and attackers are adopting several methods like social engineering, malware attacks, denial of service (DoS), etc. to launch successful attacks. Given the complexity of power grid network coupled with legacy infrastructures, it is untrustworthy to rely on the information technology-based conventional security measures. Therefore, there is a compelling need to go beyond the conventional security measures, and develop the defense-in-depth architecture to secure the SCADA grid network. In order to develop the defense-in-depth architecture, it is necessary to have the comprehensive understanding of attack processes and mechanisms. The *Cyber Kill chain* model was first introduced by Lockheed Martin analysts Eric M. Hutchins, Michael J. Cloppert, and Rohan M. Amin in 2011 [4]. It includes the sequence of stages and processes that an attacker can deploy as stepping stones to successfully execute a cyber-attack. Therefore, it assists to better understand the end-to-end decision-making process from an adversary's perspective while engaging him to create desired effects.

Log management is a next step towards developing the defense-in-depth architecture for securing the critical infrastructure. It provides efficient and secure ways to manage a network, while providing real-time situational awareness to an operator. The NIST guide to Computer Security Log Management [5] talks about the state-of-the-art SIEM software and its capabilities to perform several functions such as log storage, analysis, and monitoring. Because of its advanced capabilities and extensive features, it is preferred over the conventional log management software. The white paper by the SANS Institute [6] discusses its applications, detection processes, and also shows how to use it effectively with traditional network IDS against cyber security threats. Previously published research works [7], [8] have discussed the growing threats in the SCADA grid security, which provide a clear motivation in applying the SIEM solution for the SCADA network. However, there exist the limited substantial works which show its application in the SCADA cyber-physical environment. The paper in [9] proposes a novel framework to address the incomplete alert information to develop an efficient log management. In this paper, we have applied the open source Security Onion (SecOn), as a SIEM tool, for developing the Network System Monitoring (NSM) and rule-based IDS (RIDS) for the SCADA cyber-physical security. Specifically, we have followed the kill-chain model, which can be utilized by an advanced persistent attacker (APA), to create stealthy cyber-attacks on the power system. Later, the SecOn tool is implemented, and experimentally tested in the cyber-

[1]Acknowledgement: This research is funded in part by NSF CPS and DOE CEDS programs.

978-1-7281-0407-2/19/$31.00 

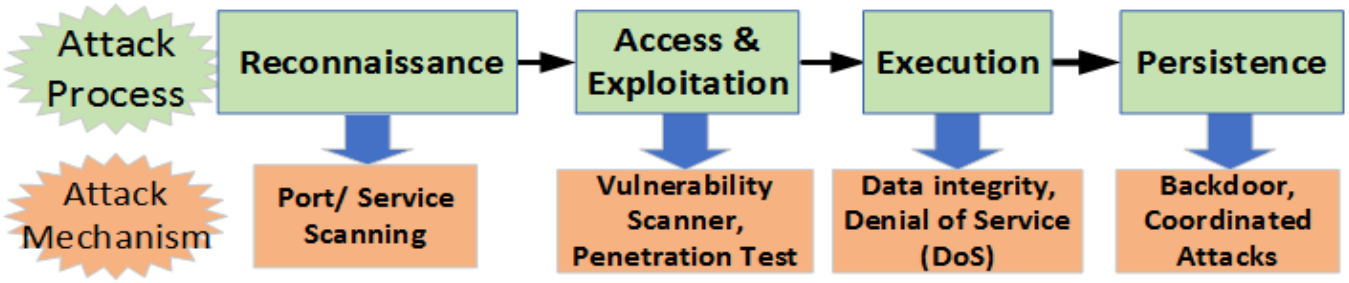



Fig. 1: Abstract level cyber kill chain model with attack processes and mechanisms.

physical environment by leveraging the resources available at PowerCyber CPS security testbed at Iowa State University (ISU). Finally, we have evaluated its performance in terms of latency and accuracy for detecting different stages of attacks in real-time.

## II. Background and Related Works

In this section, we talk about the cyber kill chain model, present related works; and discuss about the SIEM tool for developing NSM and IDS.

### A. Cyber Kill Chain

Figure 1 shows the abstract-level presentation of cyber kill chain in the context of SCADA cyber-physical security. It shows how an attacker can utilize tools, tactics, and procedures (TTPs) in a sequence of steps to deploy a successful cyber attack. Any disruption in the process/stage can break the chain, and thus, it may interrupt the attacker's objective of destabilizing the grid. There are different versions of the model which can be utilized based on the security requirements and network configuration. We have adopted a simpler version of the model as presented in [10]. The model consists of various processes/stages, which are defined as:

1. **Reconnaissance**: In this stage, the attacker tries to collect substantial and relevant information of targets to develop the blueprint of network architecture. The attacker can perform ping scanning, port scanning, service scanning, etc. as a scan attack mechanism to complete this stage. Several scanning tools like Ping Scanner, Nmap, Zenmap, etc. can be leveraged to identify alive hosts, map network addresses; and figure out the up-to-date network diagram and architecture.

2. **Access and Exploitation**: In this stage, the attacker tries to communicate or connect to a target to discover the potential vulnerabilities. Later, the obtained information about the existing vulnerabilities can be exploited to gain a foothold or the privilege escalation to launch the successful attack. The vulnerability assessment or penetration testing can be used as an attack mechanism; and tools like openVAS, Metasploit, Nessus, etc. can be utilized to complete this stage.

3. **Attack Launch/ Execution**: Before reaching this stage, the attacker must ensure that he has obtained the necessary privileges to execute or launch different types of attacks. While considering the possible attack surfaces in power system, an attack can be performed on system measurements, control signals, wide-area communication or operating field devices to disrupt the grid stability.

4. **Persistence**: This is the final stage, where the attacker creates an additional backdoor or access channel to maintain his persistence access to the compromised system, which can be exploited later for attack repetition or launching multiple attacks in a coordinated fashion.

### B. SIEM Tool: Security Onion

Security Information and Event Management (SIEM) is a combination of security information management (SIM) and security event management (SEM); and is widely deployed to provide better security log management over the network. It supports several sets of features to provide the real-time comprehensive visibility of aggregated data, crucial operational alarms to detect anomalies, and event analysis based on the aggregated logs. The paper published by the SANS Institute [11] discusses the benefits of log management; and shows how the security onion (SecOn) tool can be deployed in developing the SIEM architecture. Security onion is an open source, Linux based distribution system, which is deployed for network security monitoring (NSM), intrusion detection and prevention systems (IDPS). In general, the core functions of SecOn can be classified into three categories: 1) Packet Capturing and Monitoring, 2) Network and Host-based IDS, and 3) Packet Analysis tools.

*1) Network Security Monitoring (NSM):* NSM is a core security professional skill required for the collection, detection, log analysis, and escalation of indications and warnings to detect and respond to intrusions at the early stage. Using the network sensors, SecOn can monitor incoming and outgoing network traffic, and, hence, it provides the bird's eye view of the network to the system operator. Different analysis tools such as Sguil, Kibana and Squert can be utilized to monitor and visualize the SCADA network.

*2) Network Intrusion Detection System (NIDS):* NIDS monitors and analyzes network traffic to detect the suspicious pattern based on the assigned rules. The SecOn facilitates the sophisticated intrusion detection system (IDS) by incorporating publicly available IDS tools like BRO, Suricata, and Snort to detect different classes of anomalies in real-time. In this paper, we have focused on Snort IDS; and different set of rules are defined as well as implemented based on the kill-

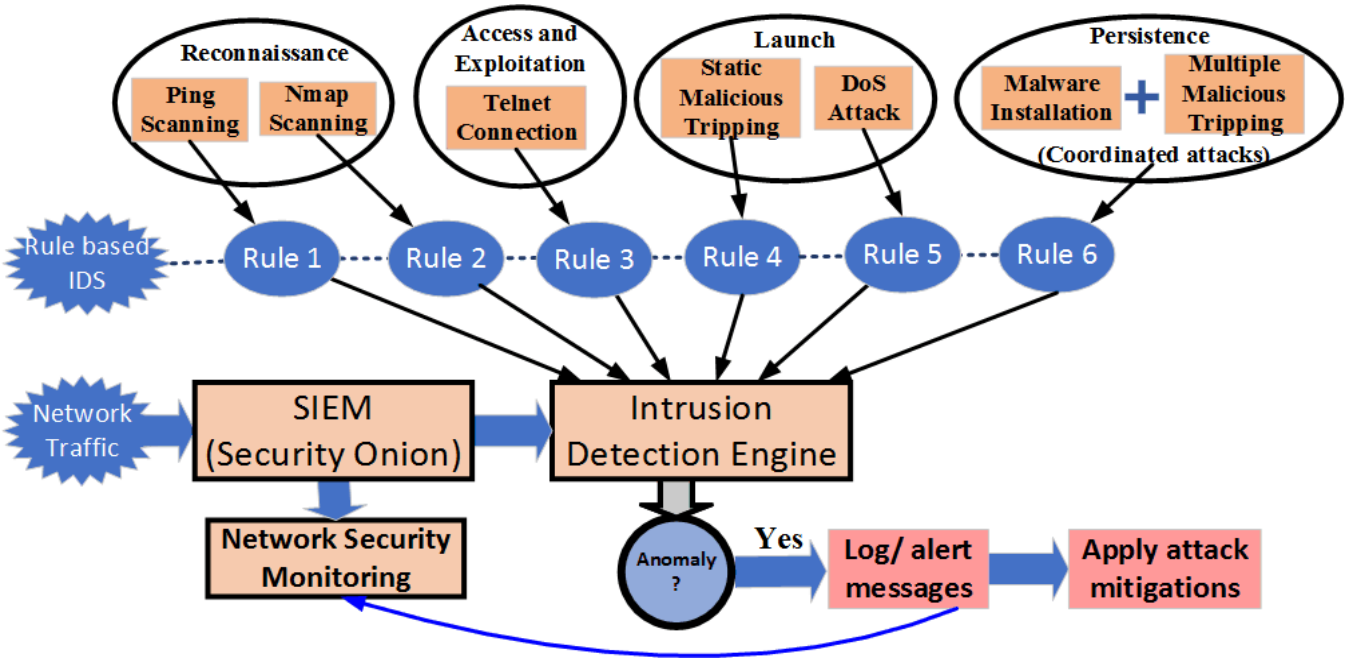



Fig. 2: Flowchart showing SIEM architecture for cyber-kill chain model

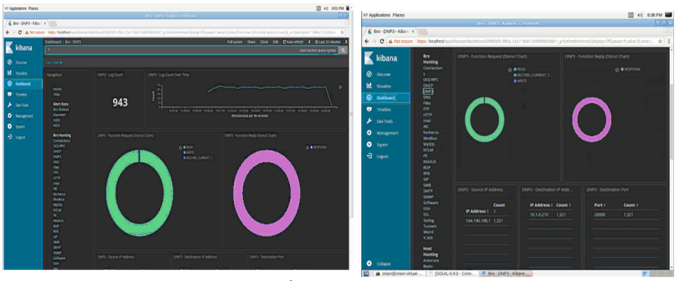
chain model. Due to the space limitation, we are not providing the detailed information about the Snort IDS.

## III. SIEM ARCHITECTURE AND IMPLEMENTATION

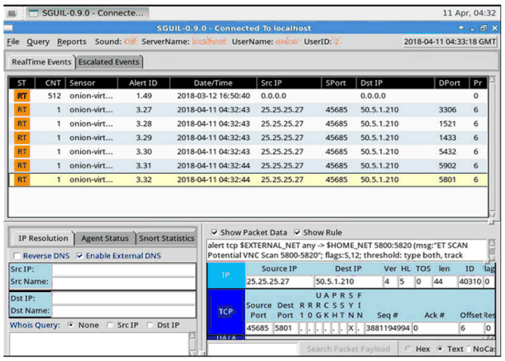
Figure 2 shows the flowchart of SIEM architecture for monitoring network packets, and detecting anomalies in real-time using the SecOn tool. The wide-area network traffic is sniffed through the SecOn, which is employed for the network security monitoring (NSM) and network-based IDS (NIDS). The NSM is performed based on the real-time packet analysis and network configuration. Figure 3 (upper figure) shows the Kibana dashboard for the DNP3 communication logs in real-time. It shows the number of DNP3 packet received over the defined time interval. Furthermore, it also provides the detailed information like source IP address, destination IP address, destination port, function codes, etc. that can also be used for advanced data analysis. Figure 3 (lower figure) shows the dashboard of Squil tool, which provides the necessary access to capture raw data, session data, and real-time events. It shows alert messages generated from the IDS based on the defined rules. For developing the NIDS, several set of rules, belonging to the different stages of chain model, are implemented in the Snort IDS. Once an anomaly is detected, the generated alert message is sent to the NSM engine for providing situational awareness to the control center operator through alert visualization and notification.

### A. Rule-based Intrusion Detection System (RIDS)

We have developed the rule-based IDS around the kill chain model to effectively detect various attacks. Since our main objective is to detect different types of attacks, irrespective of the attacker's intelligence, we have defined several rules



a) Kibana Dashboard



b) Squil Dashboard

Fig. 3: Security Onion dashboards (Kibana and Squil) for log monitoring and alert information.

that are mapped with different stages of the kill chain model as shown in figure 2. Table 1 shows the detailed information about IDS rules corresponding to different stages of attacks. In this table, rule 1 and rule 2 belong to the reconnaissance (stage 1), rule 3 belongs to the access (stage 2), rule 4 and 5 belong to the launch stage (stage3), and rule 6 falls under the

TABLE I: IDS rules for different stages of attacks

| Rules | Attack | Snort IDS Rules |
|---|---|---|
| Rule1 | Ping Scanning (Reconnaissance) | *Alert icmp $ EXTERNAL_NET any -> (IP of your substation RTU) any (msg:"ICMP to Substation"; content: "\| 10 11 12 13 14\|" ; sid: 9000547; rev:1;)* |
| Rule 2 | Nmap Scanning (Reconnaissance) | *alert tcp any any -> (IP of your substation RTU) 22 (msg:"NMAP TCP Scan";sid:10000005; rev:2; )* |
| Rule 3 | Telnet Access (Access) | *Alert tcp $ EXTERNAL_NET any -> (IP of your substation RTU) 23 (msg:"Incoming Telnet" ; content; "root" ; nocase; sid: 9000546; rev:1;)* |
| Rule 4 | DOS Attack (launch) | *Alert tcp $ EXTERNAL_NET any -> (IP of your substation RTU) 20000 (msg:"Warning DoS attack incoming"; threshold:type threshold, track by src, count 100, seconds 5; sid: 9000547; rev:1;)* |
| Rule 5 | Static Malicious Tripping (launch) | *Alert tcp !(IP from your control center) any -> (IP of your substation RTU) 20000 (msg:"Unauthorized Relay Trip" ; content :"\|00 81\|" ; rev:1;)* |
| Rule 6 | Malware installation + Multiple Malicious Tripping (Persistence) | *Alert tcp (IP from your control center) any -> (IP of your substation RTU) 20000 (msg:"Anomaly detected: 3 relays tripped under 30 sec" ; content :"\|00 81\|"; threshold:type threshold, track by src, count 3, seconds 30; sid: 9000547; rev:1;)* |

category of last stage, persistence (stage 4).

**Rule 1**: It detects ping scanning on the substation network, where a remote terminal unit (RTU) is operating. The following rule captures the incoming traffic on the specified network IP address for the ICMP protocol.

**Rule 2**: This rule generates an alert message whenever an attacker performs TCP scanning using Nmap on the substation RTU on port 22.

**Rule 3**: This rule detects the unauthorized Telnet session through a root login, which happens at port 23, to the substation RTU.

**Rule 4**: This rule detects a denial of service (DoS) attack on the substation network targeting the DNP3 communication on port 20000. It generates an alert after the first 100 SYN packets (SYN flood) during a sampling period of 5 *seconds*.

**Rule 5**: This rule detects a static malicious tripping attack, which is performed through a Man-in-the-Middle (MITM) attack between the substation RTU and control center. Digital bond has provided the rule for identifying the specific function codes [13]. We have extended the rule to whitelist the legitimate network addresses. In particular, an alert message is generated whenever the tripping command is coming from other than the control center network address.

**Rule 6**: This rule is developed to detect the last stage of chain model, persistence, where, we have assumed that the attacker has already created a backdoor access by installing a malware (Trojan horse) to compromise the control center. Once the control center is compromised, the attacker performs multiple malicious tripping attacks by switching off multiple relays with a motive to shut down the whole power grid. For this case, the previous mentioned rule will fail to detect this kind of stealthy coordinated attack as the attack is performed through the legitimate compromised device. This rule detects the attack based on the temporal behavior of control signal DNP3 packets. It computes the timing between three consecutive control signal (tripping signal) packets sent from the control center to the substation. If the computed time is less than the defined threshold, an alert message is generated. In this case, we have considered the time threshold to be 30 *seconds* for tripping three relays. However, the proper tuning of parameters has to be performed to obtain the minimum false alarms, especially during the line/relay tripping during maintenance.

## IV. TESTBED DEPLOYMENT AND PERFORMANCE EVALUATION

### A. Testbed Deployment

Figure 4 shows the experimental setup for testing the SecOn tool in the SCADA cyber-physical environment. In this work, it is configured on the substation network, where a remote terminal unit (RTU) is communicating with the control center through the DNP3 communication. The RTU is mapped with four physical relays using the IEC 61850 protocol. For implementing the attack, the installed Kali Linux machine is listening the network traffic between the control center and substation network. We have utilized the pre-installed tools, *Nmap*, and *ping* command, in the Kali machine to perform the attack reconnaissance. The DoS attack is performed by sending a huge number of random packets to the RTU through the TCP SYN flooding attack using hping tool. The malicious tripping attack is performed by listening the network traffic between the control center and substation through the Wireshark, and later replaying the captured packets using a python script. For implementing the coordinated attack for tripping multiple relays, the control center is compromised by installing a Trojan horse malware using a flash drive. Once the control center is compromised, the attacker disables the keyboard and mouse to take control over the control center; and initiates the subsequent tripping of relays, similar to 2015 Ukraine's grid hack.

### B. Performance Evaluation

We have evaluated the performance of RIDS in terms of accuracy and detection latency. Table 2 shows the high accuracy rate of six IDS rules, where the rule 1 exhibits an accurate of 99.8%, and other rules (rule 2 to rule 6) show an accuracy of 100% during the experimental testing. Figure 5 shows the latency distribution of six defined rules, which are implemented for detecting different stages of attacks. The green colored circle in each box plot represents the average of computed latency. The first two plots (a, b) belong to the attack reconnaissance, where, the computed latency is smaller

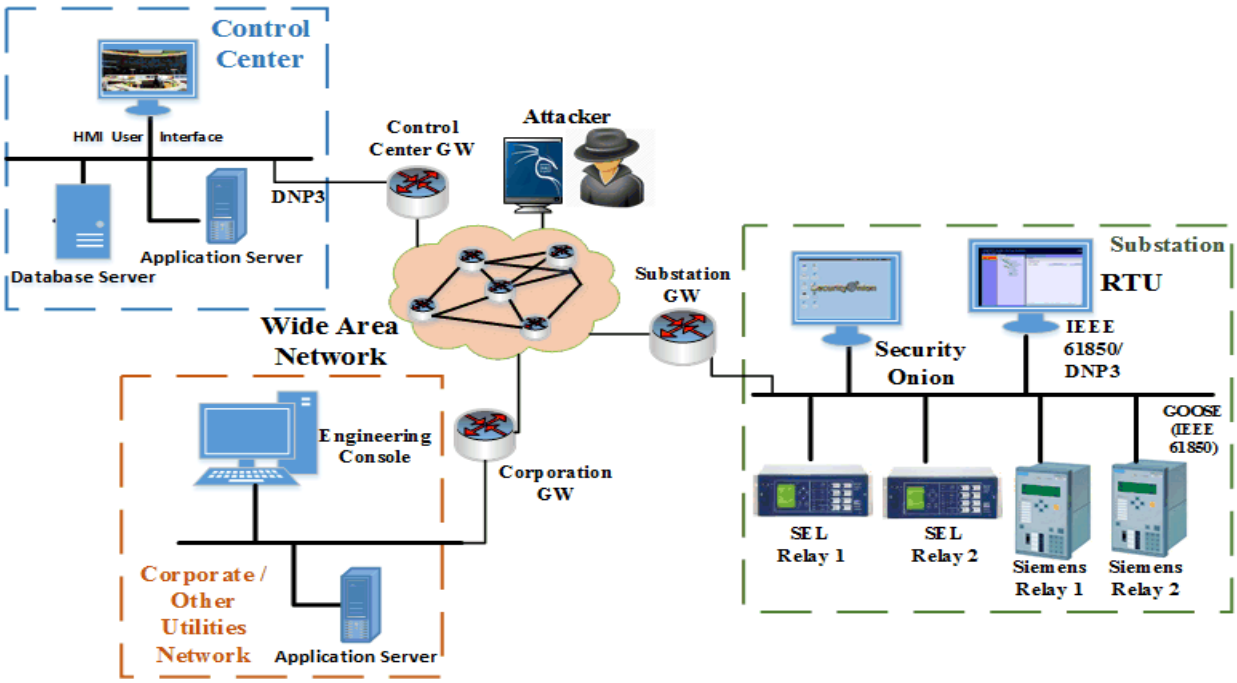



Fig. 4: Experimental setup for Security Onion (SecOn) deployment for the SIEM architecture.

TABLE II: Accuracy rate of six IDS rules

| IDS rules | Accuracy |
|---|---|
| Rule1 | 99.8% |
| Rule 2,3,4,5,6 | 100% |

for the ping scanning with an average of 1.6 seconds. The computed latency is much higher for the nmap scanning with an average of 14.45 seconds, since it performs deep and intensive scanning for a diverse set of ports, as shown in figure 5 (b). While performing the unauthorized Telnet connection, we observe a small latency varying from 0.75 seconds (minimum) to 1.44 seconds (maximum), and its average value is smaller than the ping scanning latency. During the attack execution, we have obtained the similar latency for DoS and data integrity attacks (single malicious tripping). The latency for DoS attack is uniformly distributed with an average value of around 1.5 seconds. During the single tripping attack, we have performed two attack scenarios, where, we have varied the volume of network traffic by connecting one as well as four relays between the control center and substation as shown in figure 4 (e, f). The latency for the single malicious tripping attack with 1 relay connected has an average value of 1.35 seconds. Due to the increased traffic, we have observed a relatively higher latency with an average of 1.9 seconds during the single malicious tripping attack with 4 relays connected. Finally, the multiple tripping attack is performed for the persistence stage, where 3 physical relays are tripped from the compromised control center in an interval of 1 seconds. We have successfully detected the attack with an average value of 3.588 seconds. In this case, the significant delay is observed due to the additional delay of 2 seconds while tripping all 3 relays before the IDS generates an alert message.

## V. CONCLUSIONS AND FUTURE WORKS

Security Onion (SecOn) encompasses several features and pre-installed tools, which can be leveraged to provide the unique and comprehensive solution in the development, design, and implementation of the SIEM architecture for the SCADA cyber-physical security. In this paper, we have illustrated the application of SecOn in developing the Network Security Monitoring (NSM), and rule-based Intrusion Detection System (RIDS) for the SCADA power system. For implementing the RIDS, we have deployed several rules using the Snort IDS tool for detecting cyber attacks and intrusions based on the cyber kill chain model. Finally, we have evaluated its performance in terms of accuracy and detection latency. Based on the real-time experimental analysis, we can conclude that the RIDS shows a promising performance in detecting cyber attacks with an accuracy close to 100%. Regarding the detection latency, our experimental results show that in the initial stages of kill-chain model, including reconnaissance and access, the minimum latency is obtained for the Telnet access, and maximum for the Nmap detection. In the later stages, including attack launch and persistence, similar latency is observed for DoS and data integrity attack (malicious tripping), however, the latency has increased for higher volume of traffic as well as for the coordinated attack (multiple relays tripping). In future, we will be working on the IDS research and development (R&D) to come up with a better IDS solution.

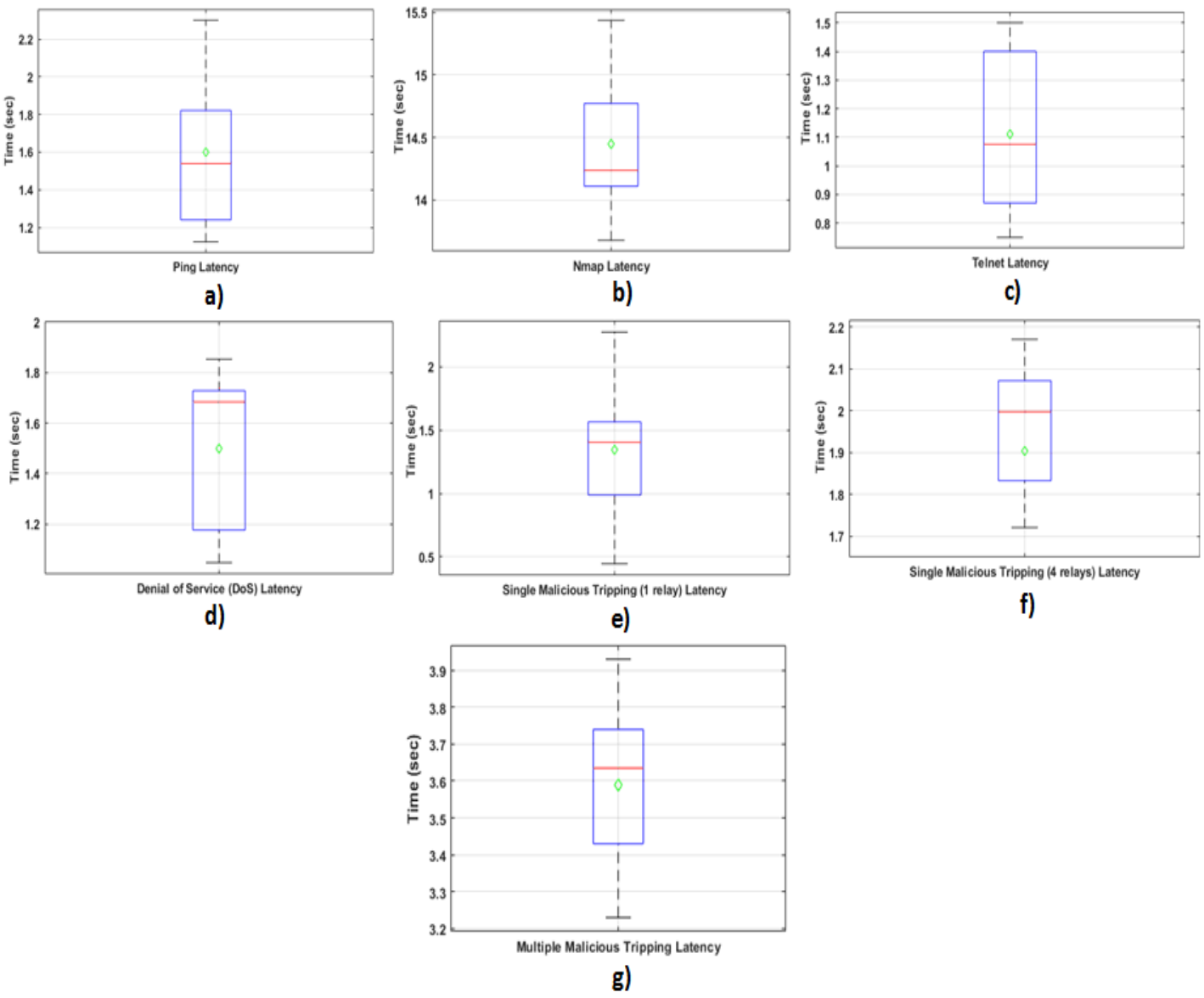



Fig. 5: Detection latency distribution for different types of attacks.

## REFERENCES


[1] "Russian Hackers Reach U.S tility Control Rooms, Homeland Security Official Say", (2018, July 23). Wall Street Journal.

[2] Industrial Control System Cyber Emergency Response Team (ICSCERT), "Monitor (ICS-MM201212)", January 2012 [Online].

[3] B. Miller and D. Rowe, A survey of SCADA and critical infrastructure incidents, Proceedings of the First Annual Conference on Research in Information Technology, pp. 51-56, 2012.

[4] M Hutchins, Eric, J Cloppert, Michael & M Amin, Rohan. (2011). Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. Leading Issues in Information Warfare & Security Research. Volume 1.

[5] K. Kent, M. Souppaya "NIST Special Publication 800–92 Guide to Computer Security Log Management", September 2006.

[6] Swift, David (26 December 2006),"A Practical Application of SIM/SEM/SIEM, Automating Threat Identification",SANS Institute. p. 3. *Retrieved 14 May 2014*

[7] A. Hahn, A. Ashok, S. Sridhar, and M. Govindarasu, Cyber-physical security testbeds: Architecture, application and evaluation for smart grid, Smart Grid, IEEE Transactions on, vol. 4, no. 2, pp. 847855, 2013.

[8] V. Kumar Singh, A. Ozen and M. Govindarasu, "Stealthy cyber attacks and impact analysis on wide-area protection of smart grid," 2016 North American Power Symposium (NAPS), Denver, CO, 2016, pp. 1-6.

[9] Blake D. Bryant and Hossein Saiedian, "A novel kill-chain framework for remote security log analysis with SIEM software", Computers & Security, vol. 67, 2017, pp. 198-210.

[10] A.C. Pappa, " Moving Target Defense for Securing Smart Grid Communications: Architectural design, Implementation and Evaluation" , M.S. thesis, Electrical and Computer Engineering, Iowa State University, Ames, IA, 2016.

[11] Sunil Gupta, " Logging and Monitoring to Detect network Intrusions and Compliance Violations in the Environment,". SANS institute 2012.

[12] V. Kumar Singh, H. Ebrahem and M. Govindarasu, "Security Evaluation of Two Intrusion Detection Systems in Smart Grid SCADA Environment," 2018 North American Power Symposium (NAPS), Fargo, ND, 2018, pp. 1-6.

[13] Digital Bond For Secure and Robust ICS.